Digital signature and hash function based approach for secure routing in VANET

A Synopsis

Submitted in partial fulfillment of registration in

Doctor of Philosophy

in

Computer Science and Applications

Proposal submitted by:

Surender Kumar

Under the supervision of:

Dr. Vikram Singh
Professor CSA

Department of Computer Science & Applications
Chaudhary Devi Lal University, Sirsa (Haryana)

CONTENTS

1. INTRODUCTION

1.1 Adhoc Network

1.2 Vehicular Adhoc Network (VANET)

1.2.1 VANET Architecture

1.3 Digital Signature

1.4 hash Function

1.5 Routing

1.5.1 Secure Routing

1.6 Dedicated Short Range Communication (DSRC)

2. REVIEW OF LITERATURE

3. RESEARCH OBJECTIVES AND METHODOLOGY

3.1 PROBLEM STATEMENT

3.2 RESEARCH OBJECTIVES

3.3 RESEARCH METHODOLOGY

4. CHAPTERIZATION

REFERENCES

1. INTRODUCTION

Wireless networks are computer networks that use radio frequency channels as their physical medium for communication (**Sarkar, 2008)**. Each node is the network broadcast information which can be received by all nodes within its direct transmission range. Since nodes transmit and receive over the air, they need not be physically connected to any network. Hence, such networks offer data connectivity along with user mobility (**Toh, 2002)**.

1.1 Adhoc Network

Wireless networks have become increasingly popular in the computing industry, since their emergence in the 1970s. This is particularly true within the last decade which has seen wireless networks being adapted to enable mobility. There are currently two variations of mobile wireless networks. The first is known as infrastructure networks, i.e., those networks with fixed and wired gateways. The bridges for these networks are known as base stations. A mobile unit within these networks connects to, and communicates with, the nearest base station that is within its communication radius. As the mobile travels out of range of one base station and goes into the range of another, a “handoff" occurs from the old base station to the new, and the mobile is able to continue communication endlessly throughout the network. Typical applications of this type of network include wireless local area networks (WLANs) **(Mohsin, 2015)**.

Mobile wireless network is the infrastructureless mobile network, commonly known as a Mobile ad-hoc network (MANET). Infrastructure less networks have no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network. Example : applications of adhoc networks are emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrains (**Mohsin, 2015)**.

1.2 Vehicular Adhoc Network (VANET)

VANET stands for vehicular adhoc network. In the VANET vehicles are taken as nodes that are connected to each other in the form of a wireless network called “vehicular adhoc network”. For transferring data between vehicles, the CBR (Constant bit rate) and TCP (Transmission control protocol) are the traffic agents used **(Kumar, 2013)**. Vehicular adhoc network is the major part of the intelligent transport system. VANET has two types of communication 1) Vehicle to Vehicle (V2V) 2) Vehicle to Infrastructure (V2I) i.e. road side unit. Vehicle to Vehicle communication uses multi-hop or multi cast technique and it uses

two types of broadcasting, first is naive broadcasting in which vehicles send broadcast message periodically and at regular intervals upon receipt of the message, the vehicle ignores the message if it has come from a vehicle behind. If the message comes from a vehicle in front, the receiving vehicles send its own broadcast message to vehicle behind it. Limitation of this broadcasting is that a large number of broadcast messages are generated. So there is risk of message collision.

Second, Intelligent broadcasting removes this message collision risk. By taking an example we can easily understand, if a car spots a dangerous road situation such as black ice, it transmits the information to the car behind it which might be heading in the direction of danger. Routing protocols are used to provide communication by routing the data among vehicles. In the VANET vehicles (nodes) themselves serve as a router. Firstly systems that will integrate this technology are police and fire vehicles to communicate with each other. The roadway system affects the life of every person as for saving the accident and for traffic management, the VANET is important in the Intelligent Transportation System (ITS) **(Agarwal, 2012)**.

VANET is a subgroup of the MANET (Mobile adhoc network). Being a subgroup of MANET,VANET has same characteristics like MANET. Nodes of both the networks are moveable so that both are mobile networks, both do not have any infrastructure and both use the nodes as a network router for routing the data among nodes or for providing communication among vehicles by forwarding the data packet. But there are some characteristics which differentiate VANET from MANET. 1) VANET, topology is very dynamically changed as compared to MANET because vehicles' speeds are high so they change the location very frequently.2) MANET nodes can be moved randomly but the VANET nodes can move in the desired fashion such as roads and highways. 3) MANET uses the GPS (Global Positioning System) to determine the position of a node but the VANET uses the AGPS (Assisted Global Positioning System) or DGPS (Differential Global Positioning System). MANET has low storage space, low battery, and processing power but these are not in VANET **(Sahu, 2013)**.

1.2.1 Vanet architecture

VANET can be implemented through integration between operators, providers and governmental authority. The architecture of a network must allow communication among vehicles and fixed roadside equipments **(Singh, 2013)**,. According to this architecture, each vehicle is composed of two types of units: (i) an on-board unit (OBU) and (ii) one or more application unit(s) (AUs). An OBU is a device in the vehicle having communication

capabilities, including at least a short-range wireless communication device dedicated for road safety while an AU is a device executing a single or a set of applications while making use of the OBU's communication capabilities. AU can be a portable device such as a laptop or PDA that can dynamically attach to (and detach from) an OBU. OBUs of different vehicles form a mobile adhoc network (MANET). OBUs and roadside units together will form ad-hoc network domain, roadside units are stationary equipments fixed alongside a road. An RSU can be attached to an infrastructure network, which in turn can be connected to the Internet. RSUs can also communicate with each other directly or via multihop. RSUs allow OBUs to access infrastructure and internet (**Lochert, 2003)**.

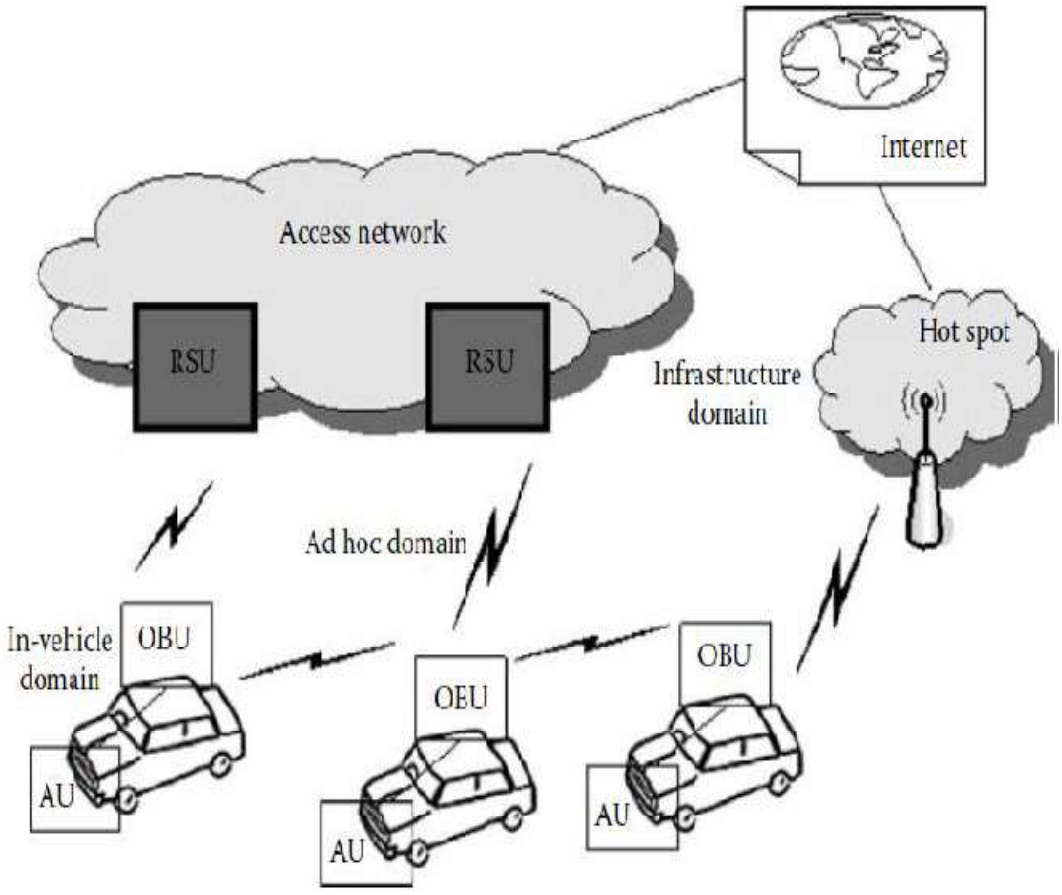

Figure.1: VANET ARCHITECTURE**(Lochert, 2003)**

1.3 Digital Signatures

Digital signatures and public key certificates are attached to safety messages for the purpose of authentication and integrity, which also can be used as tracking tokens. To help facilitate anonymity, one proposal suggests vehicle-based units should be issued multiple digital certificates, making identification or tracking of individual vehicles more difficult. This scheme is mainly based on digital signatures under the PKI (Public Key Infrastructure). Under the PKI solution, each vehicle will be assigned a set of public/private key pair. Each message sent will contain a digital signature and a corresponding certificate. Thus, the resulting message might be three times the original message.

To ensure privacy, a vehicle will have to store a large key/certificate set and frequently change keys. Each certificate contains a unique identifier, but no distinguishing information. According to the analysis by Raya and Hubaux in **(Raya, 2005)**, a vehicle should change its anonymous key within an interval of around one minute to avoid being tracked. Thus, if we assume that an average driver uses his car 2 hours per day, the number of required keys per year is approximately 43800, which amount to around 21 Mbytes. How to securely issue and store such a large number of keys will be a formidable challenge of this scheme.

1.4 Hash Function

A hash function $H : \{0,1\}^* \rightarrow \{0,1\}^n$; maps an input message m of arbitrary length to a fixed-length hash value h = H(m) of size n. If such a function satisfies additional requirements it can be used for cryptographic applications, for example in digital signatures, ID-based cryptography, and randomization of plaintexts in probabilistic cryptosystems. The primary properties that a hash function H should possess are as follows **(Gaeini, 2018)**:

- Computation of H(x) should be fast and easy, roughly linear time.
- Preimage resistance: for a given hash value h, it should be computationally infeasible to find any message m, which results in the given hash value H(m) = h.
- Second preimage resistance: for a given message m, it should be computationally infeasible to find a second message m' with m = m', which results in the same hash value H(m) = H(m').
- Collision resistance: it should be computationally infeasible to find two messages m and m' with m = m', which results in the same hash value H(m) = H(m').

Recent developments in the cryptanalysis of hash functions have clearly shown that heuristic security arguments are not good enough. Something provable is needed. Hashing is a vital

concept in cryptography and we need hash functions which are efficient and whose security can be trusted at the same time.

1.5 Routing

Routing in the computer network is an essential function, which influences both network management as the quality of services in global networks. The management of the traffic flows has to satisfy requirements for the volume of traffic to be transmitted as avoidance of congestions for decreasing the transmission delays. These two requirements, in general, are contradictory. The optimal traffic management is a key issue for the quality of the information services. Routing in networks, applying the shortest path algorithm is widely used in communication protocols in WAN (**Stoilov, 2005)**.

The efficiency of a routing algorithm depends on its performance, during congestions in the network. The routing algorithms must perform route choice and delivery of messages. The performance of the routing is assessed according to the throughput in the network (quantity of data transfer) and the average packet delay (quality of service).

- Providing multiple routes is beneficial in improving the quantity of service
- Oscillations in traffic load must be avoided but sensitivity to congestion may be significant.
- The failure of the traffic management center may be dangerous to a centralized routing management system.
- Adaptive routing with constantly updated information is helpful in avoiding congested routes.
- Quality of service, the quantity of service and speed are the three most important performance measures for any routing algorithm **(Stoilov, 2005)**.

1.5.1 Secure routing

A Mobile Adhoc Network (MANET) is an infrastructure-less, self-organizing and multi-hop network. It is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network structure. In order to facilitate communication within the network, a Routing Protocol (RP) is used to discover routes between nodes. The primary goal of such an adhoc network (RP) is a correct and efficient route establishment between a pair of nodes so that messages may be delivered on time. The wireless and distributed nature of MANETs poses security a great challenge to the system designers **(Bala, 2015)**.

A secure MANET environment should provide confidentiality, integrity, authenticity, availability, and non-repudiation. The Vulnerabilities that make MANETs highly insecure are discussed as follows **(Gupta, 2009)**:

- Dynamic nature of wireless communication.
- Node Security & tampering.
- Limited power in nodes.
- Absence of infrastructure.
- Lack of fixed network topology.

1.6 Dedicated Short Range Communication (DSRC)

Dedicated short range communication (DSRC) is a standard that aims to bring vehicular networks to North America. Traffic fatalities have been a long-standing problem in the United States, as in the rest of the world. As an indication of the severity of the problem, in 1999 there were 6,279,000 motor vehicle accidents that accounted for 41,611 deaths in the United States (**FCC, 2002)**. In 1991, the US Congress passed the Intermodal Surface Transportation Efficiency Act of 1991 that resulted in the creation of the first generation of Intelligent Transportation System (ITS). The goal of the ITS program is to incorporate technology into the transportation infrastructure to improve safety. The first generation of the Dedicated short range communication (DSRC) system operates at 915 MHz and has a transmission rate of 0.5 Mb/s. This project had limited success and was used primarily by commercial vehicles and for toll collection. One example of a first generation DSRC application is EZPass that is used for electronic toll collection.

The second generation of DSRC started in 1997 when ITS America requested that the Federal Communication Commission (FCC) to allocate an additional 75 MHz of bandwidth. In October 1999, the (**FCC, 2002)** allocated the 75 MHz of bandwidth in the 5.9 GHz band for the second generation of DSRC. Since the allocation of the bandwidth, standardized bodies have been working on the implementation details of 5.9 GHz DSRC. The North American DSRC standard program aims at creating an interoperable standard for use in the US, Canada, and Mexico. The primary goal of the project is to enable drivers to receive up-to-date information regarding their surrounding environment, thereby reducing traffic accidents. Furthermore, 5.9 GHz DSRC must have a low cost and be very scalable. In addition, the 5.9 GHz DSRC should require no usage fee from the users to access the network.

2. REVIEW OF LITERATURE

Kumar et al.(2013) has discussed Vehicular Safety Consortium (VSC), the Crash-Avoidance Metrics Partnership (CAMP) consortium and the Vehicle Infrastructure Initiative along with the giants of the light-duty vehicle manufacturers. They have also discussed developing pre-competitive safety technologies and various applications that can be offered in Vehicular Ad-hoc Networks (VANETs), a special kind of mobile ad-hoc networks where wireless equipped elements called onboard unit (OBU) in vehicles form a network with the Roadside unit (RSU) without any additional infrastructure. In this paper, they have primarily categorized various possible applications of the vehicular network, along with its features and its implementation in the real world.

Arora et al.(2014) have stressed five major categories of various Mobility Models that is Entity, Group, Urban, City-Section and Realistic Mobility models for simulation of VANET as a critical aspect in a simulation study of VANETs, that is the need for a mobility model which reflects, as close as possible, the real behavior of vehicular traffic. Their work provides a sound starting point for further understanding and development of more realistic and accurate mobility models for VANET simulations.

Sharma et al.(2013) have elicited the performance of packet delivery ratio, delay, throughput using IEEE802.11p and is compared with the values obtained for IEEE802.11. Results after analysis evince that 802.11p is much more suitable than 802.11 for vehicular communications showing better packet delivery ratio, throughput, less delay, and other advantageous improvements.

Sayana et al.(2018) have proposed a new dual authentication scheme for improving the security of vehicles that are communicating with the VANET environment. For providing such authentication in dual mode, they used two components such as hash code and fingerprint of each communicating vehicle user. Therefore, the fingerprint authentication technique was integrated into a hash code creation method in this paper to avoid malicious users to use the secret key of any VANET users in order to participate in the VANET communication. Moreover, to avoid malicious users from spoofing the authentication code issued for any VANET users and sending erroneous messages to other vehicles they have introduced a new dual key management scheme in this research paper. The dual key management scheme implemented in this paper is computationally efficient that supports secure data transmission from TA to PUs and SUs based on two different group keys, one for PUs and another one for SUs for further improving the security among different classes of vehicles. Their algorithm also takes single broadcast messages from TA to inform the group

members in order to recover the updated group key. The future development of this work is to devise new methods in order to preserve the vehicle's location privacy from the intruders.

Zhou et al.(2018) have assumed the helper is a fully trusted device, and the private key of the vehicle is generated by its helper. However, the helper is actually semi-trusted in some situations, which means that the assistant device can generate a signature without the user's approval. In this situation, 2-out-of-2 threshold manner is a considerable method to prevent the misuse of the user's secret key by the helper.

Mathew et al.(2018) have analyzed the dedicated short rang communication technique used for improved road safety with the aid of Secure Prediction Based Authentication(SPBA) scheme. They have used Beacons for secure V2V and V2R communication. When a large number of beacons arrive in a short time, vehicles are vulnerable to computation-based Denial of Service (DoS) attacks that excessive signature verification exhausts their computational resources. In contrast to most existing authentication schemes, their SPBA is an efficient and lightweight scheme since it is primarily built on symmetric cryptography. To further reduce the verification delay for some emergency applications, an SPBA is designed to exploit the sender vehicle's ability to predict future beacons in advance. In addition, to prevent memory-based DoS attacks, SPBA only stores shortened re-keyed Message Authentication Codes (MACs) of signatures without decreasing security.

Solanki et al.(2017) have proposed a novel hybrid mechanism for improving the security of MANET. In their mechanism, the security deals with the authentication and confidentiality of the data packets. The packets' information here is encoded after separating them into categories or mutable information contained in them. Authentication is performed using digital signature algorithm SHA-I. Normally the approach verifies the non-mutable information with the unique signature associated with the packet. Encryption is performed with the RSA based public key cryptosystem. Thus the approach authenticates a sender and all the intermediate nodes in a multicast environment of mobile adhoc network with a low computation overhead. The protocol assumes each node has the pre-distributed secret key. In its implementation, extensive evaluation and experimental study have proved the results' effectiveness of the suggested approach.

Gaeini et al.(2018) have proposed a new modified version of the Tillich-Zémor hash function, ZgesT, which is safer, parallelizable and practical. They have proved that ZgesT is at least as secure as the Tillich-Zémor and ZesT hash functions. In addition, by making the background mathematical problem (the factorization problem) harder, it seems the current

approaches to attack the Tillich-Zémor based hash functions can not threat ZgesT. As a disadvantage, their hash function, like other known provable secure hash functions, is slower than currently used hash functions like SHA hash functions family.

Reddy et al.(2014) have proposed a security framework called ECCEA by incorporating security aspects into the AODV protocol to provide data integrity and authentication against the adversary effects. The simulation results showed that ECCEA outperforms AODV in terms of Packet Delivery Ratio, Average End-to-End Delay, Throughput, and Normalized Routing Load for different MANET scenarios under adversary attack conditions. Their simulation results proved that the proposed ECCEA protocol outperforms the reputed AODV protocol by enhancing the Packet Delivery Ratio (PDR) from 20% to more than 85%. The simulation results also showed that the new protocol ECCEA drastically double the throughput and less Normalized Routing Load against AODV protocol under attack scenarios. The proposed security scheme, built on top of normal AODV routing protocol, achieved an overall good result. Their proposed scheme is successfully securing AODV routing protocol in defending against both malicious and unauthenticated nodes and has also proved to be more efficient and less power consuming.

Lavanya et al.(2017) have modified ECDSA, incorporating a sponge based hash function for WSN. From the results obtained through simulation, it has been found that the computation time for generating the hash code and the computation time for generating the entire signature and verifying the signature is less compared with the traditional digital signature algorithm. The performance parameters of WSN, like energy consumption, throughput, latency, and packet delivery ratio are analyzed; a better result is found from the proposed algorithm compared with the traditional authentication process.

Hafeez et al.(2013) have presented an analytical model to analyze the reliability of the IEEE 802.11p in VANETs' safety and warning applications. The analysis was based on a new mobility model in which the relationship among vehicle density, speed, and the follow-on distance rule is derived. In the analysis, several factors have been considered, such as the impact of mobility on the link availability between the transmitter and the receiver, the distribution of vehicles on the road, and the average number of vehicles within the range of the transmitter. The proposed model is built on the fact that vehicles are broadcasting their status messages within the SI and model each vehicle as a 1-D Markov chain, including the channel busy probability in every state.

Ryu et al.(2011) have given DMAE (DSRC based Multi-Channel Allocation for Emergency Message Dissemination) algorithm. DMAE allocates the highest bandwidth

channel to the urgent message firstly, and guarantees QoS between RSU and OBU through periodic channel switching. Simulation results using ns-2 shown performance improvement in terms of end-to-end delay and emergency message delivery rate.

Hu et al.(2017) have discussed that Applications of VANETs (Vehicular Adhoc Networks) have their own requirements and challenges in wireless communication technology. Although regarded as the first standard for VANETs, IEEE 802.11p is still in the field-trial stage. Recently, LTE V2X (Long-Term Evolution Vehicular to X) appeared as a systematic V2X solution based on TD-LTE (Time Division Long-Term Evolution) 4G. It is regarded as the most powerful competitor to 802.11p. They conducted link level simulations of LTE V2X and DSRC (Dedicated Short-Range Communication) for several different types of scenarios. Simulation results shown that LTE V2X can achieve the same BLER (Block Error Ratio) with a lower SNR (Signal Noise Ratio) than DSRC. A more reliable link can be guaranteed by LTE V2X, which can achieve the same BLER with lower receiving power than DSRC. The coverage area of LTE V2X is larger than that of DSRC.

Mahallen et al.(2012) have talk about the DSRC technology and its defects in order to achieve reliable content distribution. To optimize the performance of the vehicular networks, a novel network architecture using the cross-layer paradigm was presented. The architecture is called Smart Vehicular Ad-hoc Network (SmartVANET) architecture. The SmartVANET architecture can support safety, traffic management and commercial applications. The SmartVANET architecture abides by the DSRC channel plan. The architecture divides road into segments and assigns a service channel to each segment. The SmartVANET combines a segment based clustering technique with a hybrid Medium Access Control (MAC) mechanism (known as the SmartMAC protocol). Using cross-layer integration, SmartVANET also provides a solution for broadcast storm problems and offers scalability. The paper presents the SmartVANET architecture and states its advantages.

3. RESEARCH OBJECTIVES AND METHODOLOGY

The main objective of my research work is to improve the performance of DSRC protocol using digital signature and hash function cryptography algorithm with the help of Network simulator tool, NS2.35 to simulate VANET.

3.1 Problem Statement

Vehicular Adhoc Network (VANET) is a recently developed technology to achieve traffic safety and efficiency purposes through inter-vehicle communications, where the routing

protocols in VANETs play a very important role. However, one that fits all kinds of scenarios and applications does not exist for now. Insufficient forwarding nodes and network congestion can both bring severe degradation to the performance of routing protocols in VANETs. Safety and congestion are two of the biggest problems on our roads today. Is there a way to reduce accidents, save money, save lives it's called Dedicated Short Range Communication (DSRC)to improve the performance of VANET using routing protocol, we propose Secure routing protocol using two strategy of digital signature and hash function for VANET to keep the routing performance from degradation. The specific statement of the proposed research study is "Digital signature and hash function based approach for secure routing in vanet"

3.2 RESEARCH OBJECTIVES

1. To study the dedicated short-range communication standard and existing routing protocols used in vehicular adhoc networks.
2. To design a digital signature and hash function based secure routing protocol for vanet.
3. Simulating the proposed protocol using digital signature and hash function algorithm to evaluate the performance.
4. Discuss and compare the proposed protocol results with the selected existing routing protocols in vanet.

3.3 RESEARCH METHODOLOGY

- Firstly, the simulation environment is to be set up. For simulating the environment, the network simulator NS2 is used.
- Simulating the DSRC protocols using digital signature and hash function algorithms.
- The performance comparison is made with a different number of nodes, and by changing the routing protocol.
- Java programming is used to get the value from trace file and X-graph is used to generate graphs.
- Results are compared under various parameters like throughput, End to End delay, overhead and Packet delivery ratio etc.
- Discuss the result of the proposed work with existing DSRC routing protocol in VANET.

Two types of files are generated: one is scenario file and another is traffic file. Traffic can be of two types: low and high traffic and then there are two types of traffic generator like, CBR and TCP so we have four different parameters. Then the mobility model (random waypoint mobility model) is used for the simulation purpose. It represents the node movement, how their location, velocity, and acceleration change over time. The routing protocol is used for transmitting the data among nodes. After that NS2 tool is used for generating the scenario. It generates two types of files: one is **nam.filename** file and another is **tr.filename**. Nam file generates the simulation that is in actually going on and another file **tr** file has trace file format. By using awk script we can find out the value of how many packets drop, how many packets sent, how many packets received, and how much time to receive the packets.

4. TENTATIVE CHAPTER SCHEME

1. Introduction.
2. Literature review.
3. Research objective and methodology.
4. A secure routing approach in VANET.
5. Experimentation and results.
6. Conclusion.

REFERENCES

Sarkar S.K., T.G. Basawaraju and C Puttamadappa (2008), Adhoc Mobile Wireless Networks: Principles, Protocols and Applications, Auerbach Publications, 2008.

Toh. C.K. (2002), Adhoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall PTR, 2002.

Singh Abhishek, (2013), Simulation and Analysis of AODV, DSDV, ZRP in VANETs, Masters thesis in computer science and engineering, July, 2013.

Raya M. and J. Hubaux (2005), The Security of Vehicular Networks. Tech. rep., EPFL Technical Report IC/2005/009, Mar. 2005.

FCC (2002), Amendment of the commission's rules regarding dedicated short-range communication service in the 5.850-5.925 ghz band, fcc 02-302. Tech. rep., FCC, November 2002.

Sayana SS,L.M. Bernald (2018), Dual Authentication and Key Management for Secure Transmission in Vanet'' International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 04 | Apr-2018.

Zhou Yousheng , Siling Liu, Min Xiao, Shaojiang Deng (2018), An Efficient V2I Authentication Scheme for VANETs. Hindawi Mobile Information Systems Volume 2018, Article ID 4070283, 11 pages https://doi.org/10.1155/2018/4070283.

Mathew Vinitha, Prof. Leya Elizabeth Sunny (2018), DSRC: Dedicated short-range communication for improved road safety, *International Journal of Engineering Sciences & Research Technology,* ISSN: 2277-9655, January, 2018.

Sharma Kapil Dev, Sarita Singh Bhadauria (2013), Implementation of Dedicated short range communication (DSRC), IEEE802.11p in NS2 and its performance analysis over IEEE802.11, International Journal of Advance Research, IJOAR .org ISSN 2320-9119.

Kumar Vishal, Shailendra Mishra, Narottam Chand (2013), Applications of VANETs: Present & Future, Communications and Network, Volume 5, Published Online February 2013.

Arora C., K.K. Saini (2014), Survey of Various Mobility Models In VANETs published in International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 3 March 2014 Page No. 4073-4080.

Gayathri S., S.Nithya, G.Shanthini, R.Janani, R.Ramachandiran (2018), ACO-ECDSA BASED SECURE ROUTING IN VANET: A BIO-INSPIRED APPROACH published in International Journal of Pure and Applied Mathematics Volume 119 No. 14 2018, 395-406 ISSN: 1314-3395 (on-line version) url: http://www.ijpam.eu .

Kumar Vijaya, P. Inbavalli (2015), Quantitative analysis on various safety centric based approaches in VANET, (2015) Global Conference on Communication Technologies, GCCT 2015, art. no. 7342778, pp. 834-837.

Thenmozhi R., P. Karthikeyan, Vijayakumar (2015), Backtracking performance analysis of Internet protocol for DDoS flooding detection, (2015) IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2015, art. no. 7159474,

Saravanan D., V. Agalya, J. Amudhavel and S. Janakiraman (2016) , A brief survey on performance analysis and routing strategies on vanets, (2016) Indian Journal of Science and Technology, 9 (11), art. no. 89273.

Baskaran R., M. S. Saleem Basha, J. Amudhavel, K. Prem Kumar (2015), A bio-inspired artificial bee colony approach for dynamic independent connectivity patterns in VANET, (2015) IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2015, art. no. 7159384.

Agarwal A., David Starobinski and Thomas D.C. Little (2012), Phase transition of message propagation speed in delay tolerant vehicular networks, IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 1, pp. 249–263, Mar. 2012.

Sahu P., Eric Hsiao-Kuang Wu, Jagruti Sahoo (2013), Bahg: Back-bone-assisted hop greedy routing for vanet ¸are city environments, IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 1, pp. 199–213, Mar. 2013.

Lochert C., Hannes Hartenstein, Jing Tian (2003), A routing strategy for vehicular adhoc networks in city environments, in Proc. IEEE IVS, Columbus, USA, Jun. 2003, pp. 156–161.

Jiang S., Xiaoyan Zhu , Liangmin (2016), An efficient anonymous batch authentication scheme based on HMAC for VANETs, IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 8, pp. 2193–2204, 2016.

Gaeini A., M. H. Ghaffari and Z. Mostaghim (2018), An improved hash function based on the Tillich–Zémor hash function, Researchgate Res. 3 DOI:10.22052/mir.2018.97876.1078 Article June 2018.

Mohsin Ur Rahman Salfi (2015), A study of mobile adhoc networks – issues and challenges International Journal of Advanced Research in Computer Science, 6 (7), September–October, 2015,93-96.

Anuj K. Gupta (2009), Secure Routing Techniques for Mobile Adhoc Networks IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6–7March 2009.

Bala Renu, Dr. Yashpal Singh (2015), International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015, pg. 966-973.

Stoilov Todor, Krasimira Stoilova (2005), Routing algorithms in computers networks , Researchgate https://www.researchgate.net/publication/228822491 Artical January 2005.

Solanki Shelbala, Anand Gadwal (2017), Evaluation of Hybrid Security Mechanism for AODV in MANET, IJCST Vol. 8, Issue 1, Jan - March 2017.

Reddy B. Prabhakara and Dr. M.N. Giri Prasad (2014), Efficient Lightweight Hybrid Cryptography Solution to Secure Mobile Adhoc Networks, International Journal of Research in Computer and Communication Technology, Vol 3, Issue 3, March- 2014.

Lavanya M., V. Natarajan (2017), LWDSA: light-weight digital signature algorithm for wireless sensor Networks, Sadhana Vol. 42, No. 10, October 2017, pp. 1629–1643 DOI 10.1007/s12046-017-0718-5.

Hafeez Khalid Abdel, Lian Zhao, Bobby Ma, Jon W. Mark (2013), Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications, IEEE transactions on vehicular technology, VOL. 62, NO. 7, September 2013.

Ryu Min-Woo , Si-Ho Cha, Kuk-Hyun Cho (2011), DSRC-Based Channel Allocation Algorithm for Emergency Message Dissemination in VANETs, International Conference on Hybrid Information Technology ICHIT 2011: Convergence and Hybrid Information Technology pp 105-112.

Hu Jinling , Shanzhi Chen, Li Zhao, Yuanyuan Li, Baozhu Li, Yan Shi (2017), Link level performance comparison between LTE V2X and DSRC, Journal of Communications and Information Networks June 2017, Volume 2, Issue 2, pp 101–112.

Mahallen N.S., Deshmukh G.D, Raut A.S. and Totawar A.L. (2012), A DSRC based SMARTVANET Architecture, International Journal of Wireless Communication ISSN: 2231-3559 & E-ISSN: 2231-3567, Volume 2, Issue 2, 2012, pp.-35-37.